Arab Security Conference 2022

Event Schedule

Sun, Sep 18, 2022

9:00 AM

Registration

9:00 AM - 10:00 AM, Sep 18

10:00 AM

Arab Security Conference 2022 Opening Keynotes

10:00 AM - 11:00 AM, Sep 18

Main Hall

Arab Security Conference 2022 Opening Keynotes :

- Arab Security Conference 2022 Opening Video
- Dr. Bahaa Hassan Opening Keynote
-

---

5 Subsessions

● **Arab Security Conference 2022 Opening Video**
10:00 AM - 10:10 AM, Sep 18
Main Hall

● **Dr. Bahaa Hasan Opening Keynote**
10:10 AM - 10:20 AM, Sep 18
Main Hall

● **Jim Liu, Huawei Egypt CEO Opening Keynote**
10:20 AM - 10:30 AM, Sep 18
Main Hall

● **Mohamed Elashry Head Of Commercial Development at Cyshield Opening Keynote**
10:30 AM - 10:40 AM, Sep 18
Main Hall

● **His Excellency Dr. Amr Talaat Opening Keynote**
10:50 AM - 11:00 AM, Sep 18
Main Hall

11:00 AM

Surrounded by Idiots

11:00 AM - 11:30 AM, Sep 18

Main Hall

Manager…

Within dealing with Cybersecurity day-to-day work, some seriously state

that they're surrounded by idiots. Some, funnily enough, state this more often than others. And certainly, we could find many different types of problems to get along with. Some examples you might recognize; have you ever tried to reason with your stakeholders and nothing went as planned or expected? Or have you left a meeting in confusion with the feeling that you truly did not understand a single person in the room? And worst of all, some people never seem to understand what you are saying, no matter how clear you express yourself

---

Speaker

Bishoy Wasfy
GRC Director
CyShield

The Digital Signature Services & Benefits

11:00 AM - 12:30 PM, Sep 18

Blue Hall (Technical Workshops)

Technical Workshop (for Be…

the digital signature is broadly used today for the great benefits that are provided for businesses and consumers. we will demonstrate the digital signature Ecosystem and services with live demos of how to sign/verify files and how to use the Time Stamp Service.

Speaker

M

Mahmoud Elsaeed
The Root Certification authority manager
ITIDA

Hands-on Smart contract security

11:00 AM - 12:30 PM, Sep 18

Red Hall (Technical Workshops)

Technical Workshop (for Be…

Does your smart contract secure enough?

What you should learn to secure your smart contact? What are the tools you should know that will help you?

This is an on-boarding workshop for smart contract security enthusiasts. By sharing with the best practices , common vulnerabilities in smart contract and how to secure your contract against them.

Speaker

Eman Herawy
Founder
Arabs in Blockchain

11:30 AM

ICT Technologies Evolution and impact on Cybersecurity

11:30 AM - 12:00 PM, Sep 18

Main Hall

Manager…

Speaker

Medhat Mahmoud
Chief Digital Transformation officer
Huawei Technologies

12:00 PM

Building and Operating a threat-driven SOC

12:00 PM - 12:30 PM, Sep 18

Main Hall

Manager…

As businesses learn to better protect themselves, criminals are simultaneously devising increasingly sophisticated techniques to penetrate their security barriers. Attracted by the unprecedented financial rewards that cyberattacks can deliver, growing numbers of threat actors are actively seeking and targeting undiscovered security flaws. In this environment, many organizations are establishing Security Operations Centers (SOCs) to combat security issues as they arise, providing a swift response and a decisive resolution. However, the ever-growing volume, complexity, and severity of today’s cyber threats means that documenting processes, implementing basic technologies and building a team of monitoring and response specialists is just the beginning. Without the ability to continuously adapt and advance, in response to ongoing changes in the threat landscape, the effectiveness of the SOC may be compromised.

Speaker

Ahmed Ashraf
Head of Presales
Kaspersky

12:30 PM

1st Break

12:30 PM - 1:00 PM, Sep 18

1:00 PM

How DRaaS can protect from Ransomware?

1:00 PM - 1:30 PM, Sep 18
Main Hall

Manager…

Confidence comes from preparedness. Companies and admin are often found gasping for breath when they are hit by ransomware. Hence it is important to understand various aspects of a great DR plan, its readiness as well as some key configuration that is a must-do to safeguard yourself from legal, financial as well as reputational impact.

I am going to cover subtopics such as Risk Analysis, Business Impact Analysis, Building RPO/RTO strategy, Importance of the Drill, and key techniques to provide redundancy and confidence.

Speaker

Ravi Verma
Chief Technical Advisor
KLEAP Technologies

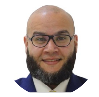
Active Directory Attacks Detection using MITRE ATT&CK

1:00 PM - 3:00 PM, Sep 18
Blue Hall (Technical Workshops)

Technical Workshop (for E…

This session aims to explain the detection of Active Directory Red teaming Operations using MITRE ATT&CK and opensource solutions (ELK Stack). During the session, we will demonstrate real-world attacks used by adversaries to attack Active Directory environments and how we can track and detect them using ELK stack queries.

Speaker



Mohammad Khreesha
Cybersecurity Director
Technawi

Red and Blue Pill in Telecom Security

1:00 PM - 3:00 PM, Sep 18
Red Hall (Technical Workshops)

Technical Workshop (for E…

We will be talking about telecommunication security, especially SIP Protocol Security vulnerabilities inside IMS and Telecom Networks such as CLI Spoofing, encryption weaknesses, and Protocol manipulation attacks and how to exploit these vulnerabilities to conduct more advanced red team operations, we will also talk about SIP interconnects between international and national telecom operators and how it can be abused by a malicious telecom operator and how these vulnerabilities may affect the national security. And we will be also demonstrating the development process of the SMSIP open-source tool which I use during SIP assessments

Speaker

Mohamed Fadel

Penetration Testing Team Leader
Security Meter

1:30 PM

Cybersecurity strategy in the digital transformation era

1:30 PM - 2:00 PM, Sep 18

Main Hall

Manager…

Speaker

Ahmed Abdel Hafez

VP For Cybersecurity
National Telecom Regulatory Authority

2:30 PM

Cyber aware in the digital era

2:30 PM - 3:00 PM, Sep 18

Main Hall

Manager…

Human beings are still the most integral part of any organization

and in the digital era People make mistakes, forget things, or fall for fraudulent practices. That’s where cyber security awareness comes in.

Speaker

Mohannad Alkalash

Founder
CYBERX

2:55 PM

Cyber Adversaries teach us in times of austerity

2:55 PM - 3:30 PM, Sep 18

Main Hall

Manager…

Most of the enterprises focus on preventing cyber attacks by relying on commercial and close-source cybersecurity products only. Currently, they use many strategies and models (e.g., zero trust) and they have many controls in place, and they can’t manage that affectively.

The key problem is a purchasing behavior by enterprises and unclear information paths. While these strategies and models are effective against some type of threats, it fails in advanced threat operations, and defenders need time to adapt these strategies that will lead to increase cost and disperse technical resources in times of austerity.

What if change the game between defenders and adversaries?!. Defenders draw real information paths and deceptive paths by iterative processes. It will help to understand adversary behaviors, adapt defensive controls and get more indicators to improve intelligence capabilities. Also, improving security teams’ critical and active thinking approaches.

During this talk, we will discuss the importance of cyber strategic planning by applying adversary engagement, also the structure of adversary engagement and the role of MITRE ATT&CK in Cyber adversary engagement analysis.

Speaker

Amgad Magdy
Strategist
SnellSec

3:30 PM

2nd Break

3:30 PM - 4:00 PM, Sep 18

Adopting DevSecOps for Containerized Apps

3:30 PM - 5:00 PM, Sep 18
Blue Hall (Technical Workshops)

Technical Workshop (for Be…

Modern SDLC is heavily depending on using containerized environments

that helps in CI/CD and application scaling. Most companies adopt DevOps which helps in improving the overall experience of SDLC. However, adopting security with each step of DevOps is crucial and this is what we call DevSecOps. During this session we will be exploring DevSecOps main activities, objectives, best practices and how to adopt and implement among your current environment

Speaker

Ahmed Abdallah
Board Member
OWASP Cairo Chapter

Introduction to Mobile Applications Penetration Testing

3:30 PM - 5:00 PM, Sep 18
Red Hall (Technical Workshops)

Technical Workshop (for Be…

This workshop will take you through the basics of Android and iOS apps penetration testing, it will teach you how to preform basic of Reverse Engineering, performing static and dynamic analysis, and identifying most known vulnerabilities that mobile application faces..

Speakers

Abdelfattah Ibrahim
Cyber Security Engineer
iSec

Mohamed Badawy
Cyber Security Engineer
iSec

2 Subsessions

● **Introduction to Mobile Applications Penetration Testing (Android)**
3:30 PM - 4:10 PM, Sep 18
Red Hall (Technical Workshops)

● **Introduction to Mobile Applications Penetration Testing (iOS)**
4:20 PM - 5:00 PM, Sep 18
Red Hall (Technical Workshops)

4:00 PM

Do you speak my language? Make static analysis engines understand each other

4:00 PM

Do you speak my language? Make static analysis engines understand each other

🕓 4:00 PM - 4:30 PM, Sep 18

📍 Main Hall

Manager…

With the widespread usage of service-oriented architectures[1 (https://www.nginx.com/blog/microservices-at-netflix-architectural-best-practices/)][2 (https://netflixtechblog.com/a-microscope-on-microservices-923b906103f4)][3 (https://eng.uber.com/service-oriented-architecture/)][4 (https://aws.amazon.com/microservices/)][5 (https://engineering.fb.com/2019/05/29/security/service-encryption/)] , detecting security issues becomes a harder task as vulnerabilities span multiple services, codebases, and programming languages.

At Meta, products and features are written in different languages - for example, the main Facebook.com codebase is written in Hack and the main Instagram.com is written in Python. These products usually need to communicate with each other or with backend systems for processing user requests.

Current security-focused static analysis tools such as CodeQL and RIPS as well as Meta-built like Zoncolan and Pysa can only analyze each codebase/language in isolation. Each tool only sees one part of the data flow, limiting the ability of application security teams to track data flows that cross the language boundary and identify security issues arising from such flows.

This presentation will introduce a novel but generic framework to exchange taint information between two or more static analysis systems and how that can be used to perform cross-language, cross-repo taint-flow analysis. It will showcase how this has been implemented inside Facebook and used at scale by Facebook's security team to detect critical security vulnerabilities spanning multiple codebases.

[1]: https://www.nginx.com/blog/microservices-at-netflix-architectural-best-practices/

[2]: https://netflixtechblog.com/a-microscope-on-microservices-923b906103f4

[3]: https://eng.uber.com/service-oriented-architecture/

[4]: https://aws.amazon.com/microservices/

[5]: https://engineering.fb.com/2019/05/29/security/service-encryption/

📢 **Speaker**

Ibrahim ElSayed
Security Engineer
Meta

4:30 PM

Workforce, The Key to Cyber Resilience

🕓 4:30 PM - 5:00 PM, Sep 18

📍 Main Hall

Manager…

📢 **Speaker**

Akash Agarwal
Vice President (IMEA & APAC)
EC-Council

5:00 PM

Lunch

🕓 5:00 PM - 6:00 PM, Sep 18

Mon, Sep 19, 2022

9:00 AM

Understanding Enterprise API Security

9:00 AM - 10:30 AM, Sep 19

Blue Hall (Technical Workshops)

Technical Workshop (for E…

We'll discuss the different design aspects to be considered for developing and maintaining enterprise APIs. We will chanell across different layers of security to ensure a proper holistic secure inclusion. From logging, traps, anomaly detection, rate limits, secure deployment, CI/CD, tokenization, fraud detection and more. We will talk about API gateways from a security point of view. This should help you better understand the requirements of properly securing your APIs

---

Speaker

Adham Fahmy

Director of Cybersecurity Services
CyShield

9:30 AM

Convergence of Security layers - Let the strategy focus on the real deal

9:30 AM - 10:00 AM, Sep 19

Main Hall

Manager…

Do we need to update our security strategies and speech? Most if the ordinary/traditional security talks strategies still approaching normal layers and missing the technology convergence and fast response needed by business

The objective of the session is helping CISO for updating their security strategies and approaching DevSecOps workflows or at least find a common ground for speaking with new IT/Development in the era of technology convergence and satisfying the business need for winning the market by fast Integrations and Developments (CI/CD).

Accordingly session will simplifying security thinking for approaching one of the DevOps components (Containers). Choosing the talk to start from Container security point view to ensure audience at least got out with proper foundation for speaking with IT/Dev team, Also choosing the core components to link the whole story to the audience from DevOps to CI/CD to Zero Trust, which are common words used these days as part of the digital transformation and high resiliency. the session will cover the containerisations concept and quick overview of NIST SP800-190 and surrounding container management tools, then will move to the view of Business to the security after the CI/CD and the impact of this on the security in a fast-base environment, and since losing the business is big impact we need to mention the remaining risks that are impacting the security specially with the convergence of IT/Dev layers which may need to converge the security layers as well and accordingly the whole mindset of think in security risks, security testing and compliance.

Speaker

Ahmed Selim

Managing Security Consultant
IBM

9:45 AM

E2E Cyber Resilient communications network

9:45 AM - 10:30 AM, Sep 19

Red Hall (Technical Workshops)

Technical Workshop (for E…

Speaker

Mohamad Madkour

huawei Egypt Cyber security officer
Huawei

10:00 AM

Security in the Fintech era

10:00 AM - 10:30 AM, Sep 19

Main Hall

Manager…

Speaker

Mostafa Menessy

Co-founder & CTO
PayMob

10:30 AM

1st Break

10:30 AM - 11:00 AM, Sep 19

11:00 AM

Cyber Crime & AML Perspective for Accounting Professionals

11:00 AM - 11:30 AM, Sep 19

Main Hall

Manager…

The progressive adoption of new technologies in the business sector impose

significant challenges for financial service professionals, compliance officers, business owners, and regulators to ensure cybersecurity in the online environment. Securing sensitive data, ensuring that it is used for legitimate purposes and are not involved in any money laundering and terrorism financing schemes is becoming increasingly crucial. The session's objective is to address these key challenges and to introduce some basic preventative actions that the professionals may adopt and perform.

Speaker

Olesya Chrysanthou

Managing Director
CPV Corporate Services Ltd

Cyber Threat Intelligence Challenges and Opportunities

11:00 AM - 12:30 PM, Sep 19

Blue Hall (Technical Workshops)

Technical Workshop (for Be…

The ever increasing number of cyber attacks requires the cyber security

and forensic specialists to detect, analyze and defend against the cyber threats in almost real-time. In practice, timely dealing with such a large number of attacks is not possible without deeply perusing the attack features and taking corresponding intelligent defensive actions—this in essence defines cyber threat intelligence notion. However, such an intelligence would not be possible without the aid of artificial intelligence, machine learning and advanced data mining techniques to collect, analyse, and interpret cyber attack evidences. In this introductory chapter we first discuss the notion of cyber threat intelligence and its main challenges and opportunities, and then briefly introduce the chapters of the book which either address the identified challenges or present opportunistic solutions to provide threat intelligence

Speaker

Ashleigh Watson

Cyber Security Director
BinZomah Technology

FinTech modern applications architecture security & DevSecOps Practices

11:00 AM - 12:30 PM, Sep 19

Red Hall (Technical Workshops)

Technical Workshop (for E…

Designing and building not only a secure modern solution (architecture) based on microservices, rich UI web app and native mobile apps but also placing the best practices of DevSecOps which assures building processes are considering security principals and controls, such as Static Application Security Testing SAST, Dynamic Application Security Testing DAST, Software Composition Analysis SCA, containers security, Runtime Application Self Protection RASP ACL, next-generation firewall NGFW

Speaker

Bahaa Farouk

Head of Engineering
Banque Misr, Digital Factory

11:30 AM

What Is Critical Infrastructure Protection (CIP)?

11:30 AM - 12:30 PM, Sep 19

Main Hall

Manager…

Critical infrastructure protection (CIP) is the process of securing the

infrastructure of organizations in critical industries. It ensures that the critical infrastructures of organizations in industries like agriculture, energy, food, and transportation receive protection against cyber threats, natural disasters, and terrorist threats.

CIP typically involves securing critical infrastructures such as supervisory control and data acquisition (SCADA) systems and networks, as well as industrial control systems (ICS) and operational technology (OT).

Speaker

Mohamed Abdelfattah

Regional OT Cybersecurity SME
Fortinet

12:30 PM

IT/OT Convergence - Jumping the Air Firewall

12:30 PM - 1:00 PM, Sep 19

Main Hall

Manager…

Many Countries and Companies today include Digital Transformation as on of its Strategies for growth. With this the rise of Digital Transformation Projects and Initiatives, comes the challenge of how to connect the Critical Infrastructure Network to the entire world to deliver digital services. That previously air gapped networks have never seen the Internet in their lives and now it is mandatory for them to remove that shield. Is it secure to connect the air gapped networks, what are the challenges and opportunities for this Convergence, Is there success or failure stories we can learn from? all these questions will be answered in this session Insha2allah.

Speaker

B

Bahaa Othman

CTO
e-serve

Who you think am i ?

12:30 PM - 2:00 PM, Sep 19

Blue Hall (Technical Workshops)

Technical Workshop (for E…

Social engineering is an attack that leverages human psychology to influence a target,

it's a broad range of malicious activities accomplished through human interactions using psychological manipulation to trick users into making security mistakes or giving away sensitive information. Cybercriminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it's to discover ways to hack your software. Generally, social engineering attackers have one of two goals whether it's for Sabotage or Theft, nowadays Over 70% of all data breaches are due to social engineering So, through this session, we will talk about the technical, tactics and procedures used in Social engineering attacks also we will talk about how red teams got benefit for these attacks and how blue teams build their defences to prevent these attacks, we are talking about how to penetrate and defend the human mind using advanced social engineering techniques that used by modern APTs.

Speaker

Muhammad Gamal Younis
Cyber Security Senior Consultant
Secure Networks

Build your skills for CTI and Defense tactics in 2022

12:30 PM - 2:00 PM, Sep 19
Red Hall (Technical Workshops)

Technical Workshop (for Be…

How can we build and grow the skills we need for Cyber Threat Intel and defense tactic playbooks in 2022? - Easy, learn the skills with Open Source tools first - 99% practical hands-on workshop with few slides.

Speaker

Wayne Burke
VP
Cyber2 Labs Inc

1:00 PM

Security Orchestration, Automation and Response - SOAR

1:00 PM - 1:30 PM, Sep 19
Main Hall

Manager…

Orchestrating the security software solutions and tools to allow the organization to streamline security operations needs a complete understanding of the SOAR that will allow to manage the incident in a proactive way by handling the threats, manage the vulnerabilities, prepare for the incident response, and security operations automation in an efficient way to achieve business goals and objectives

---

Speaker

Ahmed Fawzy
Managing Director
iExperts

1:30 PM

The Rise Of The Business-Aligned Security Executive

1:30 PM - 2:00 PM, Sep 19
Main Hall

Manager…

Today’s CISOs And Other Security Leaders Must Translate Cybersecurity Threats Into The Language Of Business Risk We live in the era of the digital business, which operates on a complex, dynamic, and highly fragmented matrix of on-premises, cloud, and hybrid infrastructure, applications, data, mobile, internet of things (IoT), and IT/OT converged systems. Every digital business must protect this sprawl of interconnected technologies that make up the modern attack surface. Yet for all the industry’s cybersecurity advances and investments, there is a massive disconnect in how businesses understand and manage cyber risk. Digital transformation has woven the threads of intellectual property and technology together. The modern CISO can no longer focus on just one thread; s/he must advocate for security of both the technology and the business — evolving from a technology expert to a business-aligned security leader.

1- Cybersecurity threats thrive amid a climate of uncertainty, making it a topic worthy of board-level visibility. Most executives (94%) say their firms have experienced a business-impacting cyberattack or compromise within the past 12 months — that is, one resulting in a loss of customer, employee, or other confidential data; interruption of day-to-day operations; ransomware payout; financial loss or theft; and/or theft of intellectual property. Roughly two-thirds (65%) say these attacks involved operational technology (OT) assets.

2- Business leaders want a clear picture of their organizations' cybersecurity posture, but their security counterparts struggle to provide one. Just four out of 10 of security leaders say they can answer the question, "How secure, or at risk, are we?" with a high level of confidence.

3- There is a disconnect in how businesses understand and manage cyber risk. Fewer than 50% of security leaders are framing the impact of cybersecurity threats within the context of a specific business risk. Only half (51%) say their security organizations work with business stakeholders to align cost, performance, and risk reduction objectives with business needs. Four out of 10 (43%) report they regularly review the security organization's performance metrics with business stakeholders.

4- Cybersecurity needs to evolve as a business strategy. This can't happen until security leaders have better visibility into their attack surfaces. Just over half of security leaders report that their security organizations have a holistic understanding and assessment of their firms' entire attack surfaces, and fewer than 50% state that their security organizations are using contextual threat metrics to measure their firms' cyber risk. This means their ability to analyze cyber risks and prioritize and execute remediation based on asset criticality and threat context is limited.

The Future Belongs To The Business-Aligned Security Leader When security and business leaders are aligned on agreed-upon contextual data, they deliver significant, demonstrable results:

1- Business-aligned security leaders are eight times as likely as their more siloed peers to be highly confident in their ability to report on their organizations' level of security or risk.

2- Most execs at business-aligned organizations (80%) report having a business information security officer (BISO) or similar title, compared with only 35% of their less-aligned counterparts.

3- Business-aligned security leaders are also more likely than their more reactive counterparts to have a defined benchmarking process: 86% have a process that clearly articulates expectations and demonstrates continuous process improvement relative to peer companies and/or internal groups, compared with just 32% of their non-aligned peers.

4- Business-aligned security leaders outpace their more reactive and siloed counterparts in automating key vulnerability assessment processes by margins of +49 to +66 percentage points.

5- 85% of business-aligned security leaders have metrics to track cybersecurity ROI and impact on business performance versus just 25% of their more reactive and siloed peers.

To achieve alignment, CISOs and other security leaders need the right combination of technology, data, processes, and people.

Cybersecurity Threats Thrive Amid A Climate Of Uncertainty We struggle to predict the future, now more than ever. Even the nature of work is shifting rapidly and without warning. But in this time of uncertainty, there is one thing enterprises can count on: Cyberthreats will proliferate, exposing every organization to significant business risk. Nearly every security and business leader says their organization had experienced a business-impacting cyberattack or compromise within the past 12 months, i.e., one resulting in a loss of customer, employee, or other confidential data; interruption of day-to-day operations; ransomware payout; financial loss or theft; and/or theft of intellectual property. Nearly half weathered five or more attacks. Further, more than two-thirds of executives say business-impacting cyberattacks have increased over the past two years — a grim trend roughly eight out of 10 executives expect will continue over the next 24 months.

Enterprises Battle Many Forms Of Business-Impacting Attacks Enterprises are not only combating a greater number of cyberattacks, but the types of attacks are more varied, with the average organization experiencing five different methods of attack. According to the executives we surveyed, fraud, data breaches, ransomware, and software vulnerabilities were among the most common types of attacks executed on enterprises over the past 12 months. Despite being just months into 2020, a surprising 41% of execs say their organizations fell victim to pandemic-related malware or phishing — making it the No. 1 mode of compromise.

Loss Or Compromise Of Data Tops The List Of Business-Impacting Events Organizations rarely emerge unscathed from a cyberattack, and respondents' organizations are no exception: Just 1% of business and security leaders say the attacks and compromises of the past year have had no impact. Cyberattacks can have a damaging impact on the business. While loss of productivity, financial loss, and identity theft are among the top consequences of attacks, over one-third of surveyed executives reported a loss of employee or customer data, and 31% experienced compromise of other confidential data.

Business Leaders Want A Clear Picture Of Their Firms' Cybersecurity Posture Security leaders are called upon to keep business leaders and board members apprised of their organizations' threat posture, but many struggle to obtain an answer to that question, let alone accurately communicate this information. Our study revealed that just four out of 10 of security leaders can answer the question, "How secure, or at risk, are we?" with a high level of confidence. Further, a whopping 66% of business leaders are — at most — only somewhat confident in their security teams' ability to quantify their organizations' level of risk or security. In the current climate of uncertainty triggered by the global COVID-19 pandemic, digital business clearly requires a new way to measure and manage cybersecurity as a strategic business risk.

There Is A Disconnect In How Businesses Understand And Manage Cyber Risk Reactive, siloed, and tactical security strategies hinder security leaders' ability to get a clear picture of their organizations' cybersecurity health and an understanding of which threats pose the greatest business risk. The study revealed a core issue: Cybersecurity initiatives are seldom aligned with business objectives. Security leaders are challenged to prioritize where they focus — not just when it comes to vulnerabilities but their entire cybersecurity strategy in general. When this strategy is disconnected from business goals, the message of risk is often lost in translation.

Business And Cybersecurity Strategies Are Seldom On The Same Page Six out of 10 business executives report their security leaders are, at best, only somewhat effective in communicating the risk cybersecurity threats pose to their organizations. So, what's the disconnect? The study revealed:

• Just 54% of security leaders and 42% of business executives say their cybersecurity strategies are completely or closely aligned with business goals.

• Fewer than half of security leaders consult business executives all the time or very frequently when developing their cybersecurity strategies.

• On the flip side, four out of 10 business executives rarely — if ever — consult with security leaders when developing their organizations' business strategies.

• Just 47% of security leaders say they always or very frequently consider business priorities when defining cybersecurity priorities.

• Fewer than half of security leaders are framing the impact of cybersecurity threats within the context of a specific business risk

Security Leaders Need To Speak The Language Of Business Risk

• "For the business leaders, money's the currency — literally and figuratively. That will [make risk] resonate for them. The technical needs to go out the window entirely. No one understands it; no one cares. They care about dollars to their bottom line."

• "[Business leaders] have the capability but not the know-how. . . They don't understand the value [of cybersecurity] unless it's in their language. They don't own the risk because they don't understand it belongs to them."

• "You need to message it to [business executives] so they receive it. At the same time, don't sell them fear — fear shuts people off. They say, 'You're full of it, you're paranoid, you're crying wolf. No way.' If you start saying, 'We probed your system and we found these holes,' that becomes real."

• "If you're going to sit in the C-suite and talk about what you're doing, if you've lined it up with what the organization has committed to being its key objectives, then that conversation will be easier."

• "If you address the high-priority business risks and align your security program with those, you're going to get a lot more buy-in from the executive team."

Security Leaders Have An Incomplete Picture Of Their Attack Surfaces And Criticality Of Assets

To be effective strategic partners to the business, security leaders must have a holistic understanding of all their entire attack surfaces within the context of business risk. And while these leaders have been given the remit to manage risk across the entirety of their organizations' critical assets, ecosystem complexity and limited visibility hinder their efforts. CONVEYING THE LEVEL OF BUSINESS RISK IS DIFFICULT DUE TO THE COMPLEXITY OF THE MODERN ATTACK SURFACE ENTERPRISES MUST PROTECT Security organizations must protect a dynamic and highly fragmented matrix of on-premises, cloud, and hybrid infrastructure, applications, data, mobile, IoT, IT, and OT systems — not to mention employees, contractors, and third-party partners. Not only did the pandemic force organizations to rethink how they do business, but it also made it even more challenging for security teams: 64% of execs say their organizations currently include remote and/or work-from-home employees in their attack surfaces. In fact, 67% of leaders are very or extremely concerned that COVID-19-related workforce changes will further increase their organizations' level of risk.

AN INCOMPLETE VIEW INTO ENTERPRISE ASSETS PREVENTS A HOLISTIC UNDERSTANDING OF RISK Limited visibility into assets beyond the traditional perimeter make it difficult for security teams to comprehensively assess risk: Employees, partners, and contractors — as well as mobile and IoT technologies — expose enterprises to considerable risk. The study found:

• While roughly 70% or more of security leaders say they have high or complete visibility into their organizations' applications, data, IT, and cloud platforms, just six out of 10 have a similar level of visibility into OT, IoT, and mobile devices.

• Six out of 10 report high or complete visibility into on-premises employees to assess risk, but only 52% can say the same when employees are remote or working from home.

• Security organizations have limited visibility to assess the risk posed by contractors and third-party partners and vendors, with just 51% and 55%, respectively, reporting high or complete visibility into these parties. As a result, few security leaders have a holistic understanding of their organizations' attack surfaces and most critical assets

Security Leaders Lack Confidence That Current Tools Can Predict Business-Impacting Cybersecurity Threats Security leaders must ensure their organizations are prepared to tackle oncoming threats, but many lack the technology, data, and processes to do so. Over half of security leaders lack confidence they have the technology or processes to predict cybersecurity threats, and roughly two-fifths are unsure they have the necessary data. This could, in part, be due to a lack of vulnerability management (VM) process automation: No more than half of security leaders say they have significantly automated VM assessment processes. Of note, only 44% of security leaders apply business risk management objectives to vulnerability prioritization practices. Additionally, three out of 10 security decision makers say their firms still primarily use manual reviews of spreadsheets to track cybersecurity performance.

Cybersecurity Metrics Often Lack Business-Risk Context Few security organizations use threat metrics that speak to business risk. At the heart of the issue is a lack of partnership between security and business leaders to ensure alignment between cybersecurity metrics and objectives with business priorities. The study revealed:

• Only half of security leaders say their security organizations work with business stakeholders to align cost, performance, and risk reduction objectives with business need.

• Four out of 10 report they regularly review the security organization's performance metrics with their business counterparts.

A Limited Approach To Benchmarking Makes It Difficult To Communicate Business Risk

Many security leaders fall short when benchmarking their cybersecurity programs against external data — or even against internal peers. Benchmarking against industry frameworks can be useful but may be highly qualitative and limited by the scope of the database used; fewer than half of security leaders consider the industry benchmarking frameworks they use to be very effective in accurately reporting on business risk. Security organizations lack consistent proficiency in benchmarking security practices. While over half of security leaders give themselves good marks for internal benchmarking practices, just 46% rate their capability to benchmark cybersecurity practices against external peers as good or excellent. Similarly, fewer than half say they are doing an adequate job benchmarking their security controls.

Cybersecurity Needs To Mature As A Business Strategy Cybersecurity cannot only be an act of activity-based defense. Today's digital business requires a new way to measure and manage cybersecurity as a strategic business risk. This new approach needs to be focused on both understanding the current risk posture and predicting the greatest threats to the business. These insights empower more informed risk-based decisions and focus security on what matters to the business. We asked security leaders to rate their security practices across various areas of oversight, technology, process, and people — areas based on a proactive, predictive approach to cyber risk that is aligned to the business.

The study found that security leaders who excel in these areas are much better equipped to speak the language of business risk. These business-aligned security leaders are 8x as likely as their more siloed peers to be highly confident in their ability to answer the question, "How secure, or at risk, are we?"

Business-Aligned Security Leaders Manage Cybersecurity As A Strategic Business Risk So what sets business-aligned security leaders apart from their more reactive and siloed peers? Our study revealed that: • BUSINESS-ALIGNED SECURITY LEADERS ARE MORE LIKELY TO ALIGN CYBERSECURITY INITIATIVES WITH BUSINESS OBJECTIVES. Business-aligned security leaders ensure their strategies are in lockstep with business priorities. They collaborate with business leaders not only to develop strategies and metrics to support organizational goals but also to inform, set, and make decisions related to business strategies. To that end, eight out of 10 business-aligned security leaders say they have a business information security officer (BISO) or similar executive to ensure each line of business works to minimize risk, maximize protection, and increase the value of the organization's business information assets.

BUSINESS-ALIGNED SECURITY LEADERS HAVE A COMPREHENSIVE VIEW OF THEIR ORGANIZATIONS' ATTACK SURFACES AND MOST BUSINESS-CRITICAL ASSETS. It's difficult — if not impossible — to accurately determine the degree to which your organization is secure or at risk without having a full understanding of your attack surface and asset criticality. Business-aligned security leaders not only are far more likely than their more siloed counterparts to have a holistic understanding of their organizations' entire attack surfaces, but they also have better visibility into the security of their most critical assets. This knowledge informs their approaches to remediation, where a combination of asset and vulnerability criticality factors into prioritizing remediation efforts.

BUSINESS-ALIGNED SECURITY LEADERS ARE MORE CONFIDENT THEY HAVE THE NECESSARY RESOURCES TO IDENTIFY AND PREDICT THREATS. Attempting to communicate business risk when you lack confidence in the tools you have at your disposal can be a futile effort. Yet few reactive and siloed security leaders are completely or very confident they have the technology, processes, and data to identify the risk level that cybersecurity threats pose to the business. Conversely, roughly eight in 10 business-aligned leaders are highly confident they are well-equipped across all three of these areas. Similarly, while more than six out of 10 business-aligned security leaders are highly confident they have the technology, processes, and data to accurately predict the likelihood of a cybersecurity threat impacting the business, fewer than half of their more reactive peers can say the same.

BUSINESS-ALIGNED SECURITY LEADERS TAKE A PROACTIVE APPROACH TO VULNERABILITY ASSESSMENT BY AUTOMATING KEY PROCESSES. Malicious actors are continuously finding new ways and opportunities to infiltrate businesses, as illustrated by the wave of COVID-19-related malware and phishing attacks. Security leaders cannot afford to sit back and react to the next attack; they must shift their approaches from reactive to proactive. Business-aligned security leaders outpace their more reactive and siloed counterparts in automating key vulnerability assessment processes by margins of +49 to +66 percentage points.

BUSINESS-ALIGNED SECURITY LEADERS WORK WITH BUSINESS STAKEHOLDERS TO ENSURE CYBERSECURITY OBJECTIVES AND METRICS ALIGN WITH BUSINESS NEED. Cyber risk management has long been measured based on tactical efforts and technical cybersecurity metrics. But to offensively manage cybersecurity risk and drive better decisions, security leaders must standardize on metrics that speak to business risk. Business-aligned security leaders don’t define metrics in a vacuum: They are six times as likely to review performance metrics with business stakeholders than their more siloed counterparts. Eight out of 10 say they partner with the business to ensure close alignment on cost, performance, and risk reduction objectives compared to just 16% of their peers.

BUSINESS-ALIGNED SECURITY LEADERS BENCHMARK BOTH THEIR INTERNAL AND EXTERNAL CYBERSECURITY PERFORMANCE. It’s difficult to gauge the maturity of your cybersecurity program if you aren’t benchmarking it both internally and against external peers. Business-aligned security leaders are more likely than their more reactive counterparts to have a defined benchmarking process: 86% have a process that clearly articulates expectations and demonstrates continuous process improvement relative to peer companies and/or internal groups, compared with just 32% of their reactive and siloed peers. This results in stronger internal and external cybersecurity benchmarking capabilities: Business-aligned security leaders outpace more reactive leaders by margins of +15 to +47 percentage points.

BUSINESS-ALIGNED SECURITY LEADERS DEMONSTRATE THE VALUE OF THEIR CYBERSECURITY INVESTMENTS. In this unprecedented climate of economic uncertainty, security leaders must also be ready to demonstrate the impact of cybersecurity investments. Strategies and practices built around understanding business risk give business-aligned leaders confidence in their ability to demonstrate the impact of cybersecurity investments. Most business-aligned security leaders are very or completely confident in their ability to demonstrate that their cybersecurity investments are positively impacting their business performance compared with just over half of their more reactive and siloed counterparts. This confidence is, in part, rooted in their use of metrics to track cybersecurity ROI and impact on business performance.

Recommendations

1- Communicate clearly and with confidence. A whopping 66% of business leaders are — at most — only somewhat confident in their security teams’ ability to quantify their organizations’ level of risk or security. However, business-aligned security leaders are eight times more likely than their siloed counterparts to be highly confident in their ability to answer the question, “How secure, or at risk, are we?”

2- Align cybersecurity initiatives with business objectives. Enlist a BISO or equivalent executive in collaborating with the leaders of each line of business to develop strategies, goals, and metrics to maximize the protection of business information assets. Organizations that have tight alignment between business and security are 2.3 times more likely to have a BISO or similar executive.

3- Benchmark both internal and external relative cybersecurity performance. Articulate expectations about cybersecurity performance and demonstrate continuous process improvement relative to both peer companies and internal groups. A limited approach to benchmarking makes it difficult to gauge cybersecurity performance. Business-aligned security leaders are more likely than their more reactive counterparts to have a defined benchmarking process: 86% have a process that clearly articulates expectations and demonstrates continuous process improvement relative to peer companies and/or internal groups, compared with just 32% of their peers.

4- Prioritize vulnerability assessment by automating key processes. Prioritization based on business risk context will help focus your efforts. You can accomplish this by automating vulnerability assessment processes — including monitoring and incorporating threat intelligence and applying business risk management objectives to vulnerability prioritization practices utilizing a predictive approach — and by conducting vulnerability assessments on a frequent basis using automated tools. Business-aligned security leaders are 3.3 times more likely to use a combination of asset criticality and vulnerability factors when prioritizing remediation efforts. Such leaders are also seven times more likely to automate the application of business risk management objectives to vulnerability prioritization practices.

5- Develop a comprehensive assessment of the organization's most business-critical assets. A robust prioritization strategy for business impact mitigation requires a holistic understanding of the organization's entire attack surface, including remote workers, OT, and cloud deployments, as well as insight into which assets pose the greatest business risk if compromised. Business-aligned security leaders are 3.3 times more likely than their more siloed counterparts to have a holistic understanding of their organizations' entire attack surfaces.

6- Define metrics to demonstrate the value of cybersecurity investments. Few security organizations use threat metrics that speak to business risk. At the heart of the issue is a lack of partnership between security and business leaders to ensure alignment between cybersecurity metrics and objectives with business priorities. Gain confidence to demonstrate the value of cybersecurity investments to business leaders by cultivating and consuming cybersecurity metrics for both ROI and the impact on business performance. Businessaligned security leaders don't define metrics in a vacuum: They are six times as likely to review performance metrics with business stakeholders than their more siloed counterparts. Eight out of 10 say they partner with the business to ensure close alignment on cost, performance, and risk reduction objectives compared to just 16% of their peers. And 85% of business-aligned security leaders have metrics to track cybersecurity ROI and impact on business performance versus just 25% of their more reactive and siloed peers.

📢 **Speaker**

Mohamed Sadat
M.sadat

2:00 PM

2nd Break

🕑 2:00 PM - 2:30 PM, Sep 19

2:30 PM

Decipher Vendors Language and Govern your Cybersecurity Program using Cyber Defense Matrix Model

🕑 2:30 PM - 3:00 PM, Sep 19

📍 Main Hall

Manager…

Cyber Defense Matrix is a new framework developed by Sounil Yu,

it has many revolutionary angles to build, map and tune cybersecurity programs. It also demystifies the vendor buzzwords and branding claims to on ground controls that can be mapped to any organization. In this session, we will go through the framework from different angles and show its benefits and numerous use cases for CISOs, CIOs and risk assessors.

📢 **Speaker**

Wessam Maher
Chief Information Security and Risk Officer
The American University in Cairo

Data Protection Laws in the Middle East and GDPR

🕑 2:30 PM - 4:00 PM, Sep 19

📍 Blue Hall (Technical Workshops)

Technical Workshop (for E…

Most of the constitutions stipulate the need to protect private life, and that the protection of privacy must be stipulated by the laws of the state, and it is not permissible to impose any censorship on the means of communication, telephone conversations, or messages without reasoned judicial permission.

The laws generally provided for the protection of personal data, in penal laws, civil laws, child laws, and central bank laws, but recently, specifically in 2016, the general data protection regulation was born, which entered into force in 2018, and the GDPR is the regulation for the protection of personal data The most strict in the world for its critical details and heavy fines, tech giants have recently been among their biggest victims of heavy fines for the breaches of their provisions.

Since then, data protection laws have become the talk of the hour and the most important file on the table of governments, parliaments, and even companies.

Governments began enacting laws to protect personal data, and companies began to pay close attention to governance and compliance with data protection laws.

The paper will focus on personal data protection laws in two ways:

1- The first aspect is the governance and compliance procedures that are required of companies, especially the Startups that seek to expand in many countries.

2- The necessary procedures for countries to ensure the proper application of personal data protection laws and the amendments to be added in addition to cooperation protocols between countries, some of which are within the scope of cross-border data.

The importance of the paper for Startups is that they are interested in the rapid expansion of the same business model without looking at data protection laws in other countries. For example, financial technology companies under the supervision of the Central Bank come out of the scope of application of the Egyptian Personal Data Protection Law, but when they expand to another country, they find that they may enter the same model under the data protection laws in that country, in addition to the judicial scope of the application of the European Regulation for Companies that Expand in European countries or dealing with data of EU citizens.

The paper will come up with recommendations within the scope of the startups' vision on their ability to comply with the data protection law in Egypt or their departure from the scope of its application in other countries, and the extent to which companies can reconcile internal data protection laws and in other countries while building their own business model.

Finally, the proposed amendments to data protection laws are in accordance with the state's vision to support the digital economy.

Speaker

Eslam Mezar

Partner
Mezar Law Office

3:00 PM

5G Security

3:00 PM - 3:30 PM, Sep 19

Main Hall

Manager…

5G attack scenarios and how to apply countermeasures Tackling Security Challenges in 5G Networks

Speaker

Hassan Naguib

Sr. Manager Cyber Security Engineering
Orange Egypt

3:30 PM

The perfect sniping location: Hunting threats of Air and Interconnect attacks within NFV environments

3:30 PM - 4:00 PM, Sep 19

Main Hall

Manager…

A conclusive view over the methods of threat hunting for Air and Interconnect attacks, discussing the structures of such attacks, their threat modelling scenarios and how to detect and treat them within both traditional telecom and NFV environments.

📢 **Speaker**

Mohamed Noseir
Senior Cyber Security Program Manager
RSA Security

4:00 PM

Zero Trust, Why now and What's Next ?

🕓 4:00 PM - 4:30 PM, Sep 19
📍 Main Hall

Manager…

Zero Trust is the most popular topic in any cloud discussion. Its no

more an option but a must to survive in your cloud journey. Is it a new concept ? Technology ? How and why should we implement it ? Any best practices ? How can we take it further and what is the future outlook for Cloud Security. Please join me in a interactive session discussion Zero trust and the myth behind the cloud security in 2022.

📢 **Speaker**

Ahmed Nabil
Mr

4:30 PM

Arab Security Conference 2022 Closing Ceremony

🕓 4:30 PM - 6:00 PM, Sep 19
📍 Main Hall

Arab Security Conference 2022 Closing Ceremony :
Arab Security Conference 2022 Closing Keynotes :
Omar ElSherbiny Head of Strategic Accounts at Cyshiled
Arab Securtiy Cyber Wargames 2022 Champions
Arab Security Awards Ceremony 2022

6:00 PM

Lunch

🕓 6:00 PM - 7:00 PM, Sep 19